DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 23 February 2009

IMSE-KNX-IMO

23 February 2007

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 2-07 – Data-at-Rest Protection for Mobile Computing Devices (MCDs)

1. References.

a. Memorandum, Chief Information Officer (CIO)/G-6 (SAIS-GKP), 28 Sep 06, subject: Army Data-at-Rest (DAR) Protection Strategy.

b. Army Best Business Practice (BBP), Data-at-Rest (DAR) Protection, Mobile Devices using Encrypting File System (EFS) Implementation, 12 Oct 06.

c. Message, VCSA, 271600Z Oct 06, subject: Army Data-at-Rest (DAR) Protection Strategy, ALARACT 209/2006

d. Message, VCSA, subject: OPSEC Notice to Army Leaders (ONTAL) 06-01.

2. Background. The Army continues to lose sensitive information due to negligence in protecting data on MCDs and removable media. These losses place the lives of Soldiers at risk. Therefore, the Army has set forth requirements for encrypting information on all MCDs and removable storage devices. The MCDs are defined as laptops, tablet-PCs, portable notebooks, USB hard drives, USB thumb drives, and similar systems.

3. Responsibilities. Commanders/Directors, Information Management Officers (IMOs), and Information Assurance Security Officers (IASOs) must be proactive in ensuring users are trained and mobile devices configured for protection from existing and emerging threats that include the following:

a. Opportunistic theft. The loss of an MCD primarily to an individual interested in monetary value or resale of the device without other motives.

b. Dedicated agent or "hacker." The loss of an MCD to an individual with the intention of compromising potential information contained on the MCD, ransoming the device for profit, or leveraging the MCD for their own use.

c. State-sponsored terrorist or foreign agent(s). The loss of an MCD to an individual(s) with dedicated resources and motives to target specific users and MCDs for the information contained on an MCD.

4. User requirements training. The DAR BBP, which contains instructions for the configuration and training, is at https://knoxdoim815/portal/user_training.htm. Upon completion of training, the user must send the IMO/IASO an e-mail stating: "I have read and understand the Army's Best Business Practice for Data-at-Rest (DAR) Protection." The IMO/IASO will keep the e-mail on file.

a. All MCDs and removable storage devices must have the following:

(1) Label. "Complies with Army Data Encryption Policy and Authorized for Travel." (FK Form 5078, Data-at-Rest (for laptops) and FK Form 5078a, Data-at-Rest (for thumb drives).

(2) Configure properly using the Encrypted File System.

b. All travelers must be trained on the following:

(1) What data must be encrypted.

(2) How to encrypt data.

(3) How to protect data and MCDs from loss or theft

(4) What to do in the event an MCD is lost.

5. Reporting. When all MCDs have been configured and labeled and the users trained, the commander/director must send a digitally signed e-mail to tamela.plamp@us.army.mil.

6. Point of contact is the Installation Information Assurance Manager at 624-5782.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A